PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/14, 9/32 — A1

(11) International Publication Number: WO 98/29983

(43) International Publication Date: 9 July 1998 (09.07.98)

(21) International Application Number: PCT/AU97/00887

(22) International Filing Date: 30 December 1997 (30.12.97)

(30) Priority Data:
PO 4417 30 December 1996 (30.12.96) AU

(71) Applicant *(for all designated States except US)*: COMMONWEALTH BANK OF AUSTRALIA [AU/AU]; 48 Martin Place, Sydney, NSW 1155 (AU).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: MAPSON, Michael, Joseph [AU/AU]; 69 Yalor Road, Bangor, NSW 2234 (AU).

(74) Agent: WATERMARK PATENT & TRADEMARK ATTORNEYS; Unit 1, The Village, Riverside Corporate Park, 39–117 Delhi Road, North Ryde, NSW 2113 (AU).

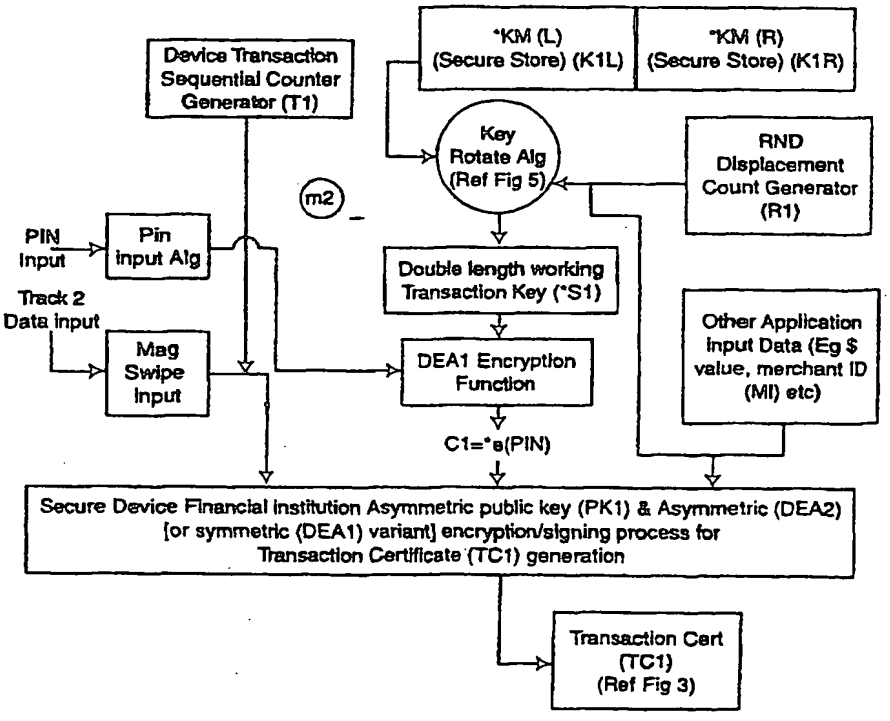
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: TRANSACTION KEY GENERATION SYSTEM

(57) Abstract

The present invention relates to the generation of an encryption key for a message to be transmitted over a communications network, where there is no real time link between the encryption and decryption devices. Without limitation, one application of the present invention is in financial transactions between a customer, vendor and financial institution. In essence, the present invention stems from the recognition that if the transactions are not necessarily to occur in real time nor in an environment of total security in transmission, then the transaction must be considered as unidirectional from the customer (or their device) to the issuer. Thus, from the customers end, a unique key is generated for each transaction, preferably without reference to external devices. In one form, the unique key protects in particular, a PIN or the like provided by the cardholder. However, the device issuing institution will be aware of the basic encryption key for each device, and when coupled with further data (in the illustrative case a random number input to a rotation or other rearrangement algorithm), the issuer can recover the correct key and decrypt this protected part of the transaction identification block. Also two unidirectional transactions may form a bidirectional transaction session.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

TRANSACTION KEY GENERATION SYSTEM

Technical Field

The present invention relates to the generation of an encryption key for a message to be transmitted over a communications network, where there is no real time link between the encryption and decryption devices. Without limitation, one application of the present invention is in financial transactions between a customer, vendor and financial institution.

Background Art

Electronic messaging systems of various types have come into increasing use over the last decade. Such developments as widespread use of internal networks, and the increase of internet access and use, have contributed to this growth.

Electronic messaging is traditionally carried out using one of several mechanisms. In one type of arrangement, exemplified by electronic funds transfer, all terminals are uniquely identified, the communication lines are considered insecure, and transaction keys are generated for each transaction using real time on-line links between the terminal and the host. However, such a system is not suitable where messages may be received out of order, as in a packet based system, and/or where communications real-time links may be unreliable.

Another alternative is the use of asymmetrical key encryption, such as RSA, in which a public key is disseminated, with the private key held only by the intended receiving party. A corresponding relationship needs to be established to allow for two-way communications. In such systems, the same key is used for numerous transactions, which creates a security risk over time - in other words, the key is not unique to any given communication.

It is an object of the present invention to provide an encryption system which allows for an encryption key to be generated for each message, but where there is no real time link required between the sender and the receiver.

It is further object of the present invention to provide an encryption system which allows regeneration of the message encryption key by an authorised recipient, using data from the message.

Summary of the Invention

According to a first aspect, the present invention comprises a system for encrypting and decrypting a message, the encrypting means comprising an encryption engine, and a random or pseudo-random number generator providing a numerical input to said engine, said engine in response to the numerical input generating a unique transaction key, said key being used to encrypt a message and incorporate the encrypted form in a message block, said message block further including said numerical input as unencrypted data, said decryption means being adapted to produce a corresponding decryption key from said random number and thereby decrypt said encrypted message.

In essence, the present invention stems from the recognition that if the transactions are not necessarily to occur in real time nor in an environment of total security in transmission, then the transaction must be considered as unidirectional from the customer (or their device) to the issuer. Thus, from the customers end, a unique key is generated for each transaction, preferably without reference to external devices. In one form, the unique key protects in particular, a PIN or the like provided by the cardholder. However, the device issuing institution will be aware of the basic encryption key for each device, and when coupled with further data (in the illustrative case a random number input to a rotation or other rearrangement algorithm), the issuer can recover the correct key and decrypt this protected part of the transaction identification block.

Also two unidirectional transactions may form a bidirectional transaction session.

A further aspect which is in contrast to existing electronic payment systems is that merchant data will, at least to some extent, need to be supplied to the cardholder for inclusion in the encrypted transaction identification block. Merchant data allows identification of the merchant. As the intermediary parties play no part in the encryption, the data will have to be provided to the cardholder (customer) device for encryption. Some of this data may have to be attached to the transaction identification block in a non secure environment, there may also be provided verification of this within the encrypted part.

In a still further aspect, the present invention is directed to a method of effecting a financial transaction as herein disclosed.

Preferably, the encryption is performed using an encryption engine contained within a secure hardware element of the transmitting means. For example, the transmitting means may comprise a secure card reader in combination with the customer's credit or debit card, and a PC or similar device connected to a modem. Preferably, the message block further includes a unique identifier for the secure encryption means, and the decrypting device has access to the specific encryption engine used for that device, so that input of the numerical input allows the key to be re-generated separately at the decryption means. This provides a unique key for each message without the necessity for a real time link.

Preferably, the encrypted data further includes a unique transaction identifier, generated from a predetermined set by the encryption means. Each encrypted message will have a unique transaction number. The decryption means stores a set of at least those transaction numbers which have been used. If a decrypted message contains an invalid or previously used transaction number, it can be identified as a duplication or replay of another message - further enhancing the system security.

The present invention is particularly applicable to systems such as the internet, and more particularly to arrangements in which a secure transaction may pass through several parties before being presented to the intended recipient. An example of such an application is a payment instruction from a party to purchase goods via the internet. The fundamental relationship to effect the payment is between the customer and the financial institution which will pay the vendor. Hence, the customer may send a message block to the vendor, including unencrypted data such as the amount, the customer's financial institution, and the date, together with an encrypted confirmation of these details and confidential details such as a credit or debit card number, a PIN (personal identification number), the amount (to alleviate tampering of the transaction value by an intermediary or the merchant) and the customer's account details. The vendor may pass the message block to a bank or financial institution for

later submission to the customer's bank. Alternatively, if the transaction has a small value, the vendor may store the message blocks and submit them as a batch to a bank or similar financial institution, preferably in pseudo real time for later processing. In either case only the issuing bank and the customer have access to the relevant encryption and decryption data. Also, as the key is a transaction key, and indeed the underlying encryption function is preferably unique to a given encryption means, even if a single message is intercepted and decrypted by some means, the key for only that transaction will be obtained. Even if the encryption means is subverted, the keys used for all other encryption means will remain secure.

Other applications of the inventive system will be apparent to the reader.

Thus, the present invention provides for a transaction key to be generated, without a handshake between the encrypter and decrypter.

Brief Description of the Drawings

One illustrative embodiment of the present invention will now be described with reference to the accompanying figures, in which:

Figure 1 is a schematic overview of a general arrangement in which the present invention may be used;

Figure 2 is a block diagram illustrating one possible encryption process in the transmitting device;

Figure 3 is an example transaction certificate format;

Figure 4 is an example of a block message format; and

Figure 5 illustrates an exemplary algorithm for generating a transaction key.

Detailed Description

The present invention will be described with reference to a particular application, that of funds transfer over a communications network such as the internet. However, it will be understood that with suitable modifications the present invention is more broadly applicable. The design and details of the encryption system, and receiver and transmitter elements, are not essential in detail to the present invention - it is only their functionality which defines the present invention. Greater or lesser levels of encryption security may be used depending upon the wishes of the system implementer.

Furthermore, where # (hash) is referred to in the following text, it may preferably consist of, but not be confined to, any cryptographically robust One Way Function (OWF), such as, for exemplary purposes only AS2805 OWF, or Secure Hash Standard (SHS), HAVAL or MD Series.

Referring to figure 1, the arrangement shown is one in which a domestic customer wishes to purchase goods or services from a cyber merchant - e.g. one accessible via the internet. The home user has a magnetic stripe or smartcard credit, debit or customer card, a secure device card reader, and a PC and modem connected conventionally for internet access. The other parties shown are the merchant, which is the vendor; the acquirer, which is the financial institution with whom the merchant has a relationship; the card issuer, who has a relationship with the customer; and the device issuer, who supplied the secure device card reader. It will be appreciated that less complicated arrangements are possible where, for example, the device issuer is the card issuer, or the merchant and customer share the same financial institution.

A typical debit purchase transaction may operate as follows:

1. Customer selects item(s) for home purchase from the merchant's web site, and initiates purchase software between the merchant's site and the home PC. An applicable software "shopping" application exists, with hooks to import and export data to a Secure Device attached to, for example COM2. The import / export control between the application and the Secure Device will be a separate control protocol.

2. Customer has a mag stripe, linked or smartcard debit card.

3. Merchant provides purchase details - for example, merchant ID, value of transaction, and other relevant data. The merchant ID is transported securely (eg SSL) between the merchant's web site and the customer, for inclusion in the purchase certificate (TC1).

4. Customer purchase software confirms debit and requests card reading / swipe. The secure device checks for correct reading of the card.

5. Customer purchase software initiates "GetPIN" to secure device, which encrypts and stores the entered clients PIN.

6. Secure device concentrates encrypted PIN results with other transaction data. An advancing or other suitable transaction number is assigned - this may be simply 1, 2, etc, or selected from a more complex predefined set. Concatenated result is cryptographically incorporated into a transaction certificate using a second encryption process. An illustrative transaction certificate is shown in figure 3. This encryption may be, for example, using the public key of an asymmetrical key pair, issued by the device issuer. The secure device is capable of PIN encryption possibly with symmetric double length keys and is capable of encrypting multiple data blocks with a stored protected asymmetric 'n' bit modulus Secure Device Issuer public key half. The 'n' bit modulus may be 1024 bit, or other as considered suitable. Alternatively, the asymmetric encryption process may be replaced with a symmetric encryption process using a variant key derived from a base key and the random number.

7. Assembled purchase transaction is sent to the merchant, e.g. via email or Internet, see Figure 3 & 4.

8. The transaction may be stored by the merchant for batching into a set of transactions for upload to the acquirer institution. A transaction transfer protocol is designed or exists to satisfy these requirements.

Note: The Merchant Acquirer may or may not have issued the customer Secure Device reader and / or the customer mag stripe card. In this scenario, it is assumed that the Acquirer has issued neither. Thus, where the Merchant Acquirer has issued one or both the reader or card, simplification of these steps is possible.

9. The acquirer determines, from for example unencrypted information in the message block, which institution issued the secure device sourcing the transaction. The transaction message provides a Secure Device identifier to be contained within external plain text data, as well as within the certificate.

10. The transaction is forwarded to the secure device issuer, for certificate data recovery, using existing (INTERCHANGE) interbank secure communication systems.

11. The secure device issuer decrypts the certificate data and checks the transaction number against a transaction number database indicating the possible transaction numbers for the device, and which of those transaction numbers have been used. If the transaction number has been used, the device issuer will send a message indicating an error or duplication to the acquiring institution. The entire recovered transaction is now sent to the acquirer, for normal processing and exchange with the issuing institution. The acquirer will then advise the merchant whether funds are cleared or not. The secure device issuer can verify the transaction certificate and check for device transaction duplication (replay) in the transaction number database. The checking application will record the current transaction in the database so it too cannot be duplicated and recover the transaction in an SCM (card no., $val, etc).

12. The process proceeds as an existing interchange transaction, via the Acquirer. The secure device issuer can return (interchange) the reconstructed message data to the Acquirer for standard interchange processing.

13. The merchant is informed if the funds are to be forwarded or not. A funds failure mechanism exists to provide the merchant with payment "OK" or "Rejected".

It will be appreciated that many of the elements of the system are already in use, and hence will not be explained further in detail. For example, interbank communications may proceed as normal - the only change is the requirement for involvement by the device issuer. Purchase software is already widely utilised for internet shopping - the only modification required is to ensure adequate security and controls between the software and the secure device. Similarly, the secure device may be merely a simplified version of the card readers currently used for POS transactions.

A key feature of the present invention is that the secure message is assembled by the customer's secure device, not the merchant, with a unique identifier for the secure device and for the transaction, as well as the usual PIN inserted by the customer. The probity of intermediaries is not crucial to a secure transaction occurring. The present invention enables the device issuer to identify the source of the message, and verify that replay or duplication of the

transaction has not occurred, without any direct communication between the secure device and the device issuer. Moreover, no acknowledgment needs to be sent to the issuer's customer, other than a normal statement entry in due course. Moreover, the transaction certificate may also be used as a specific transaction ID, for example as an invoice number, between the customer, the merchant, the device Issuer and the funds Issuer, for audit or reconciliation purposes. Even if transactions occur out of order, for example transaction 15 is received by the issuer after transaction 16, the transaction can still proceed and be confirmed as valid - this is not possible with conventional EFTPOS systems.

The transaction described above relates to debit transactions - however, it could be applied to credit transactions, or to any other process where it is essential to confirm that the data originated from the correct source, as well as keep the data itself secure, but real time connection is not always possible. Examples include medical and insurance data, confidential reporting and negotiable security instructions.

The present invention fully supports current standards for the interchange of financial institution data, and provides a complete audit trail with key regeneration capability.

The merchant data is preferably sent to the customer using appropriate encryption established between the merchant and the customer.

There are two relevant forms of encryption. They are Symmetric & Asymmetric respectively.

Symmetric Keys - General

Symmetric encryption uses a common shared key between two parties.

The DES algorithm (Data Encryption Standard - DEA1), has been the accepted means of symmetric encryption, within the Financial Industry.

DES has traditionally used Single Length (8 byte / 64 bit) keys, of which 56 bits are actually used in the encryption process. Because of increases in attacking computer power, single length keys must be extended to double length, using a modified encryption process. The double length key is split into components called Key Left and Key Right.

A double length key is denoted by an asterisk, e.g. *KM1. (This example shows Double length Masterkey number one).

Secure Device Encryption Process

Referring to Figure 2, the top two boxes of this diagram show the device master key. It is a *Master Key. The key is loaded into secure device storage and cannot be recovered or read back outside the device.

PIN Encryption Process for UATEKS

The device *Master Key, **(*KM)** is loaded by the Secure Device ISSUER. When required to encrypt an entered PIN, the key is passed through a non linear modification algorithm, seeded by random value. **(R1).**

The resultant derived *Transaction Key **(*S1)** encrypts the PIN:

$C1 = *_e(PIN) = *_{fn(R1,*KM)}$.

The encrypted double length result, C1, together with the random seed, (R1), is passed to and stored by the Transaction Certificate generator.

Device Transaction Tracking Process

Each Secure Device will produce a sequentially incremented device transaction number **(T1).** TI cannot be read in plain text prior to transaction certificate encryption. It can only be recovered by the Device Issuer host, during transaction verification. The device transaction number size will be of sufficient length to allow a reasonable time span of events to be recorded for replay checking and velocity checking at the host databases. The counter is never reset and only advances in value. At the end of its cycle life, sufficient time will have elapsed for the host database to recognise that roll-over to , for example, 00000000 is a reasonable event for that particular device.

Each transaction value of (T1) is placed in the Certificate generator.

Magnetic Swipe Track 2 Data

Any transaction will require the user to swipe a card for Track 2 or other relevant data to be captured. The data may also be captured from another source, for example a smart card data file.

Track 2 contains all pertinent data to determine account details. It is protected by placing the **entire** track 2 data within the Transaction Certificate generator.

Transaction Certificate Generator

Asymmetric Keys

The secure Device will use an asymmetric key half, (PK1), which may be termed the PUBLIC key component.

In reality, this key component need not be public and can be stored, in device secure storage, along with the device master key.

The transaction certificate generator is an asymmetric encryption algorithm within the card reader device. The asymmetric key half (PK1) used to produce the certificate is treated, in the device, as a secure generic key, unique to the Secure Device Issuer.

Note 1: Each Secure Device could have its own unique asymmetric key set. However, this is a waste of resources when the "Public" half of the key can be protected in the same way that the unique device *Master Key is stored. This removes the need for "PK1" certification. Device unique keys would also require additional Issuer host storage space.

Note 2: Alternatively each Secure Device PK1 could be delivered, from the reader device, to an associated terminal PC, together with the assembled content of the generator (Figure 3 illustrates an example TC1 Format). This might permit faster transaction certificate assembly. It would also support a case for a device unique PK1. However, this is not a preferred method and would greatly reduce the security of the transaction, potentially allowing fund values and Merchant ID etc to be altered.

Note 3: If an asymmetric PK1 is impractical, it is possible to use a symmetric derivative variant of the base key, to produce a signing key in lieu of PK1.

The transaction certificate, TC1, can only be recovered by the Secure Device Issuer. Thus, ALL transactions must come through the device Issuer, before the transaction can be placed into conventional Interchange, for processing.

This would allow selling transactions back to other card issuers, if the Secure Device Issuer were not the Card Issuer as well.

Figure 4 illustrates an example of both a symmetric and asymmetric block message format.

Secure Reader device

The reader device may be purpose built or may be existing technology. The reader can be constructed with a security processor chip capable of operating to industry standards. The encryption processing can be capable of both DES and asymmetric operation. Preferably, the asymmetric key length moduli is 1024 bits. A fixed timing block of output of results may be provided. Device power control etc may be activated by any suitable means, for example DSR or RTS type combinations or similar signals from associated equipment.

Key Rotation Algorithm

Referring to Figure 5,

Base Key *KM: (Reference numeral 1) Consists of a device unique key, 128 bits long. This key is programmed by the Issuer, into each device and also stored securely in the Issuer OCRF database, protected by a domain master key. (Conventional process). The key is recalled for each PIN decryption process, to derive the transaction key(s) for the current transaction.

Random Generator (R1)L & (R2)R: (Reference numeral 2) The combined random components R1 and R2 are each a minimum of 64 bits long. *S1 is thus decoupled from *KM for additional protection against known cryptanalysis attacks, etc. The combined 16 byte resultant value is transmitted in the plain text message sent to the Issuer.

Hash Function (#Fn): (Reference numeral 3) Each #Fn may be, but not necessarily, functionally identical. The 128 bit device key *KM is hashed to 64 bits using the left and right (R1)L and (R2)R components respectively. Each 64 bit product is denoted #1L and #2R in Figure 5 schematic. Each 64 bit hash product is then concatenated to produce the final 128 bit transaction key S1 (reference numeral 4) required by the encrypt function to produce C1 (ΣPIN) in Figure 2.

Suitable modifications and alternatives to key lengths, algorithms and other terms, functions or the embodiments and examples given, as would be considered suitable by those skilled in the art, without departing from the generality of the disclosure of the present invention, are to be included within the scope of the present application.

THE CLAIMS DEFINING THE INVENTION ARE AS FOLLOWS:

1. A system for encrypting and decrypting a message, the encrypting means comprising an encryption engine, and a random or pseudo-random number generator providing a numerical input to said engine, said engine in response to the numerical input generating a unique transaction key, said key being used to encrypt a message and incorporate the encrypted form in a message block, said message block further including said numerical input as unencrypted data, said decryption means being adapted to produce a corresponding decryption key from said random number and thereby decrypt said encrypted message.

2. A system for effecting a financial transaction in an environment which lacks a relatively high level of security, including

a key generator, issued by an acquirer or an Issuer, which generates a unique key for each transaction without reference to external devices, and

a customer card which includes PIN and other relevant details which is encrypted by the customer device and transmitted via a transaction identification block, wherein

the basic encryption key for each customer device is known by the issuer, and therefore the issuer can recover the correct key and decrypt the relevant part of the transaction identification block.

3. A method of effecting a financial transaction in an electronic payment systems, comprising:

suppling from a merchant to a customer device, merchant data for identifying the merchant, in consequence of trade between the merchant and a customer, and

the data being included in an encrypted transaction identification block.

4. A method of effecting a debit purchase transaction, including the steps of:

a. Customer selects item(s) for home purchase from the merchant's web site,

b. Customer has a mag stripe, linked or smartcard debit card.

c. Merchant provides purchase details to customer device, for inclusion in a purchase certificate (TC1).

d. Customer device confirms debit and requests card reading / swipe.

e. Customer device initiates "GetPIN" to secure device, which encrypts and stores the entered clients PIN.

f. Secure device encrypts PIN and concatenates result with other transaction data,

g. a transaction number is assigned

h. assembled purchase transaction is sent to the merchant,

i. the transaction is sent to the acquirer,

j the acquirer determines which institution issued the secure device sourcing the transaction from a Secure Device identifier contained within the data,

k. the transaction is forwarded to the secure device issuer, for certificate data recovery.

5. The method as claimed in claim 4, further including the steps of:

l. the secure device issuer decrypts the certificate data and checks the transaction number against a transaction number database indicating the possible transaction numbers for the device, and which of those transaction numbers have been used to determine whether the transaction is to be valid or rejected,

m. the merchant is informed if the funds are to be forwarded or not.

6. An encryption method and device which allows regeneration of the message encryption key by an authorised recipient, using data from the message, as herein disclose

7. A device, system or method as herein described.

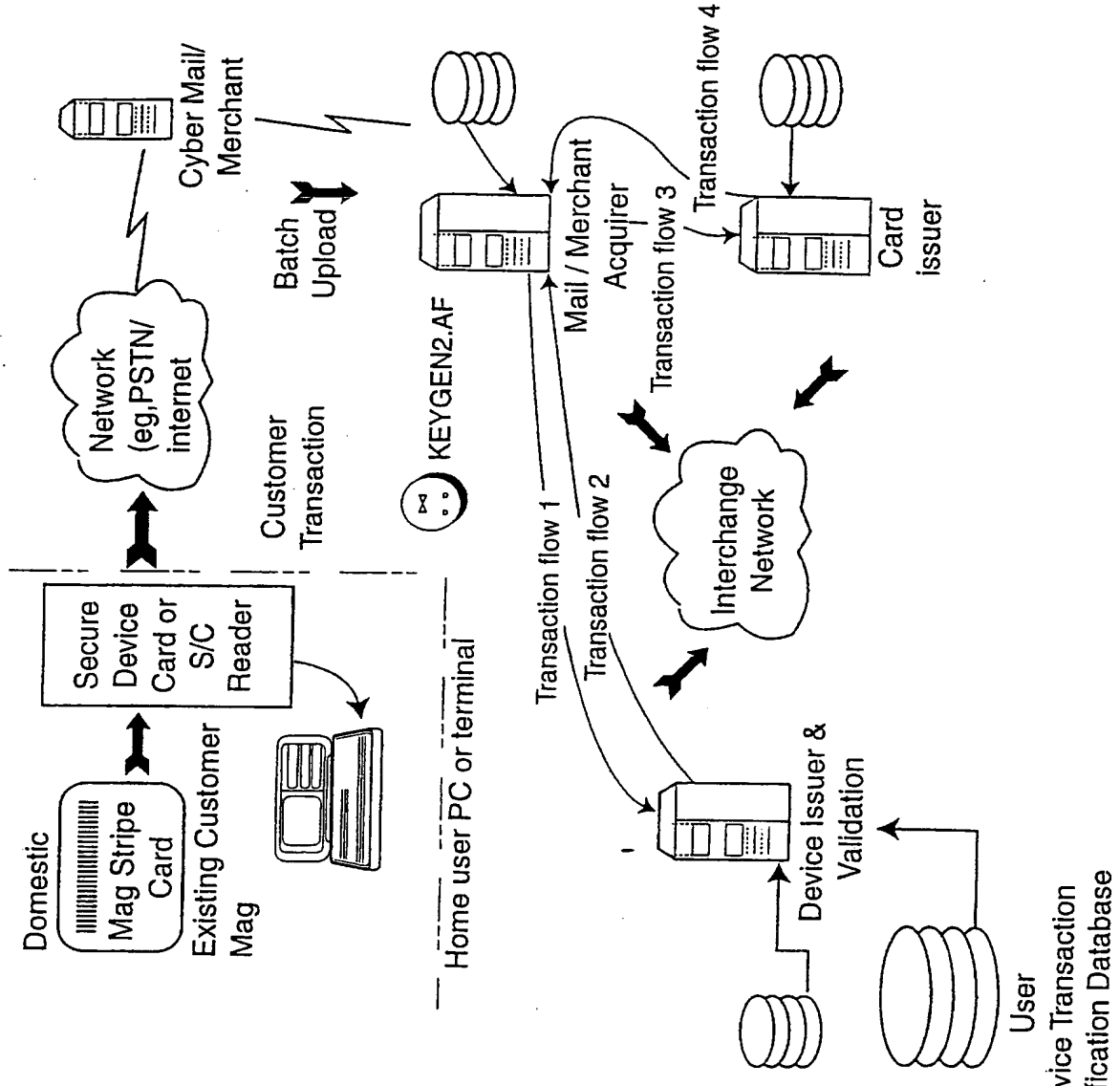


Fig 1.

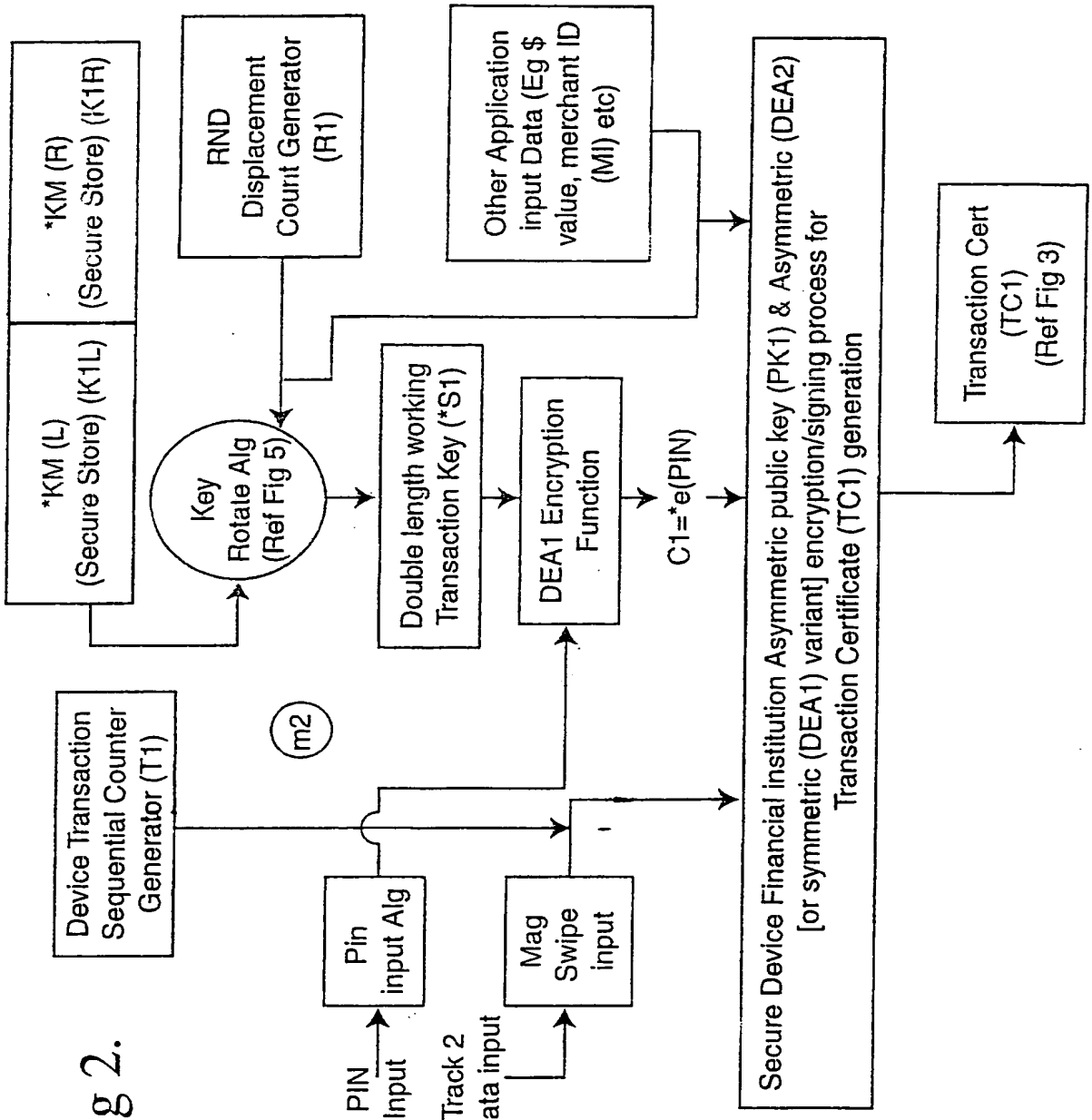


Fig 2.

Fig 3.

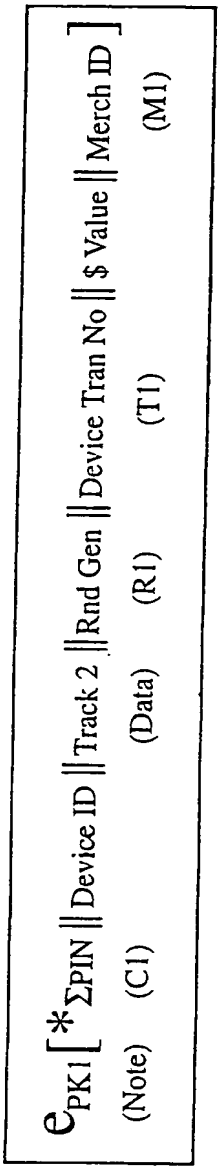


Fig 4.

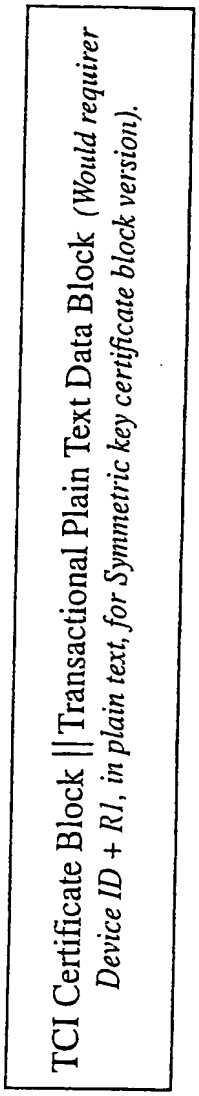
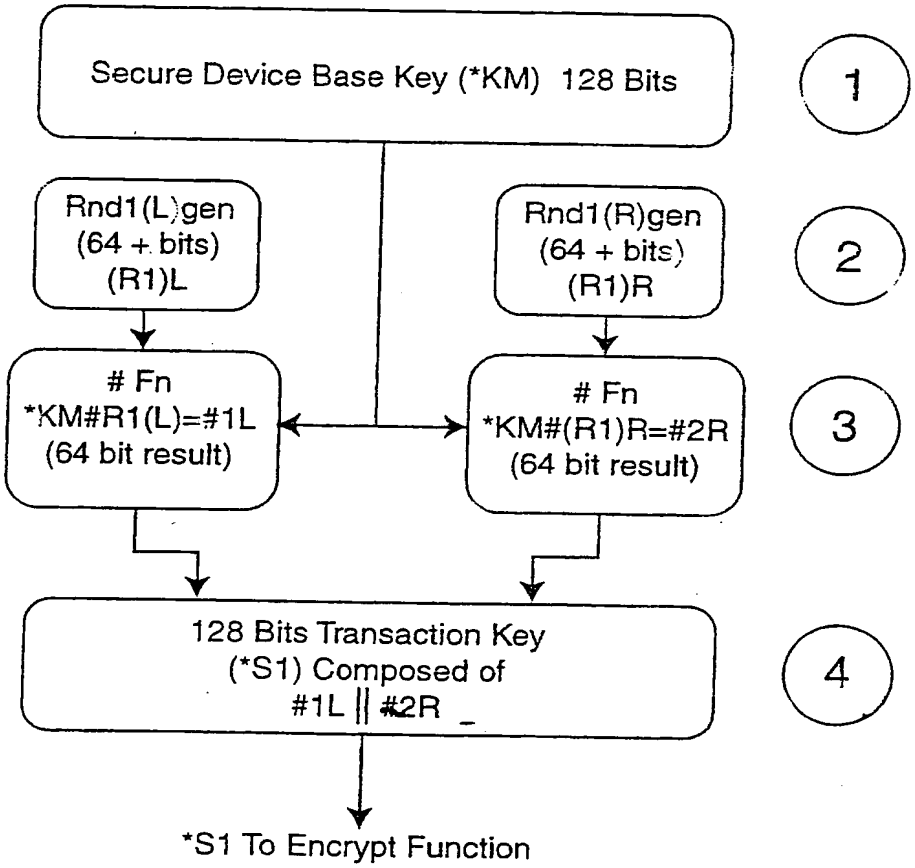


Fig 5.


Secure Device Base Key (*KM) 128 Bits
1
Rnd1(L)gen
(64 + bits)
(R1)L
Rnd1(R)gen
(64 + bits)
(R1)R
2
Fn
*KM#R1(L)=#1L
(64 bit result)
Fn
*KM#(R1)R=#2R
(64 bit result)
3
128 Bits Transaction Key
(*S1) Composed of
#1L || #2R
4
*S1 To Encrypt Function

INTERNATIONAL SEARCH REPORT

International Application No.
PCT/AU 97/00887

A. CLASSIFICATION OF SUBJECT MATTER

Int Cl[6]: H04L 9/14, 9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L 9/14, 9/16, 9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
IPC: AU as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
DERWENT:WPAT

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,A	WO A 97/16902 (TRI-STRATA SECURITY, INC.) 9 May 1997	
A	WO A 88/01817 (UNISYS CORPORATION) 10 March 1998	
A	US A 5478994 (RAHMAN et al.) 26 December 1995	

☐ Further documents are listed in the continuation of Box C

☒ See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 February 1998	04.03.98
Name and mailing address of the ISA/AU AUSTRALIAN INDUSTRIAL PROPERTY ORGANISATION PO BOX 200 WODEN ACT 2606 AUSTRALIA Facsimile No.: (02) 6285 3929	Authorized officer J.W. THOMSON Telephone No.: (02) 6283 2214

INTERNATIONAL SEARCH REPORT
Information on patent family members

International Application No.
PCT/AU 97/00887

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member			
WO	97/16902	AU	23639/97		
WO	88/01817	US	4782529	US	4809327
US	5478994	US	5627355		

END OF ANNEX

SDOCID: <WO___9829983A1_I_>